06-01-00

CERTIFICATE OF EXPRESS MAIL
NUMBER EL 548524796 US
DATE OF DEPOSIT May 30, 2000

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Atty. Dkt. No.: KINS:002USC2

Prior Application Examiner:
Bali, V.

BOX PATENT APPLICATION
Assistant Commissioner for Patents
Washington, D.C. 20231

Classification Designation:

Prior Group Art Unit: 2723

REQUEST FOR FILING CONTINUATION APPLICATION UNDER 37 C.F.R. § 1.53(b)

This is a request for filing a continuation application under Rule 53(b) (37 C.F.R. § 1.53(b)) of co-pending prior application Serial No. 08/940,553 filed January 31, 2000, entitled "POINTING DEVICE WITH BIOMETRIC SENSOR" which is a continued prosecution application (CPA) of U.S. Patent Application Serial No. 08/940,553 filed on September 30, 1997 (abandoned) and having the same title.

☒ 1. Enclosed is a copy of the prior application Serial No. 08/940,553 as originally filed, including specification, claims, drawings, power of attorney and declarations. The undersigned hereby verifies that the attached papers are a true copy of the prior application as originally filed and identified above, that no amendments (if any) referred to in the declaration filed to complete the prior application introduced new matter therein, and further that this statement was

made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statement may jeopardize the validity of the application or any patent issuing thereon.

(a) ☒ The inventorship is the same as prior Application Serial No. 08/940,553.

(b) ☐ Deletion of inventor(s). Signed statement attached deleting inventor(s) named in the prior application, see 37 C.F.R. § 1.63(d)(2) and 1.33(b).

(c) ☐ Priority of foreign patent application number , filed in is claimed under 35 U.S.C. § 119(a)-(e). The certified copy:

☐ is enclosed.

☐ has been filed in the prior Application Serial No.

☒ 2. Enclosed is a check in the amount of $789.00 to cover the filing fee as calculated below and the fee for any new claims added in the Preliminary Amendment referred to in Clause No. 8 below.

CLAIMS AS FILED IN THE PRIOR APPLICATION
LESS CLAIMS CANCELED BELOW

FOR	NUMBER FILED	NUMBER EXTRA	RATE	FEE
Basic Fee				$345.00
Total Claims	52 - 20 =	32 X	$9.00 =	$288.00
Independent Claims	7 - 3 =	4 X	$39.00 =	$156.00
Multiple Dependent Claim(s)				$.00
		TOTAL FILING FEES:		**$789.00**

☒ 3. Applicant is entitled to Small Entity Status for this application.

☐ (a) A small entity statement is enclosed.

☒ (b) A small entity statement was filed in the prior nonprovisional application and such status is still proper and desired.

☐ (c) Small entity status is no longer claimed.

☒ 4. If the check is missing or insufficient, the Assistant Commissioner is hereby authorized to charge any fees under 37 C.F.R. §§ 1.16 to 1.21 which may be required for any reason relating to this application, or credit any overpayment to Fulbright & Jaworski Deposit Account No. 50-1212/KINS:002:USC2/BAM.

☒ 5. Enclosed is a copy of the current Power of Attorney in the prior application.

☒ 6. Address all future communications to:

Michael C. Barrett
FULBRIGHT & JAWORSKI
600 Congress Avenue, Suite 1900
Austin, Texas 78701
(512) 418-3000

☐ 7. The prior application is presently assigned to _____.

☒ 8. Enclosed is a preliminary amendment. Any additional fees incurred by this amendment are included in the check at No. 2 above and said fee has been calculated after calculation of claims and after amendment of claims by the preliminary amendment.

☐ 9. Cancel in this application claims of the prior application before calculating the filing fee. (At least one original independent claim must be retained).

☐ 10. Amend the specification by inserting before the first line the sentence: --The present application is a continuation of co-pending U.S. Application Serial No. 08/940,553 filed September 30, 1997--.

☐ 11. Enclosed are formal drawings.

☐ 12. An Information Disclosure Statement (IDS) is enclosed.

☐ (a) PTO-1449.

☐ (b) Copies of IDS citations.

☐ 13. Transfer the sequence information, including the computer readable form previously submitted in the parent application, Serial No. filed , for use in this application. Under 37 C.F.R. § 1.821(e), Applicant states that the paper copy of the sequence listing in this application is identical to the computer readable copy in parent application Serial No. filed . Under 37 C.F.R. § 1.821(f), Applicant also states that the information recorded in computer readable form is identical to the written sequence listing.

☐ 14. Other:

☒ 15. Return Receipt Postcard (should be specifically itemized).

Respectfully submitted,

Michael C. Barrett

Michael C. Barrett
Reg. No. 44,523
Attorney for Applicants

FULBRIGHT & JAWORSKI
600 Congress Avenue, Suite 1900
Austin, Texas 78701
(512) 418-3000

Date: May 30, 2000

CERTIFICATE OF EXPRESS MAIL
NUMBER EL 548524796US
DATE OF DEPOSIT May 30, 2000

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: David J. Kinsella	Prior Group Art Unit: 2723
Prior Serial No.: 08/940,553	Prior Examiner: Bali, V.
Filed: Concurrently Herewith	Atty. Dkt. No.: KINS:002USC2/BAM
For: POINTING DEVICE WITH BIOMETRIC SENSOR	

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Applicant respectfully requests that the above-identified patent application be amended as follows prior to examination. Applicant submits that the foregoing amendments more particularly point out the subject matter of the invention.

No fee is believed necessary, but Applicant grants authorization to withdraw any and all appropriate fee(s) under 37 C.F.R. §§ 1.16 to 1.21 from Fulbright & Jaworski Deposit Account No. 50-1212/KINS:002--2/BAM.

Favorable reconsideration of the application in view of the following amendments and remarks is respectfully requested.

AMENDMENT

Please make the following amendments:

In the Specification:

On page 1, line 9, please add the following: -- The present application is a continuation of co-pending U.S. Patent Application Serial No. 08/940,553 filed January 31, 2000 entitled, "Pointing Device with Biometric Sensor," which is a continued prosecution application (CPA) of U.S. Patent Application Serial No. 08/940,553 filed on September 30, 1997 (abandoned) and having the same title. Pending Application Serial No. 08/940,553 is incorporated herein by reference in its entirety. --

In the Claims:

Please cancel claims 3-6 and 25-48 without prejudice or disclaimer.

1. (Amended) A pointing device comprising:

an interface for operably communicating with an electronic system;

a position sensor, responsive to user movement thereof, for conveying [user] positional information by way of said interface to the electronic system;

a user-depressable button for conveying [user] selection information by way of said interface to the electronic system;[and]

a biometric sensor disposed at a location such that when operating said pointing device in a normal manner a user's hand rests naturally in a position to place a finger of the user's hand in proximity to and readable by said biometric sensor[, said location equally well suitable for use by either a right-handed or a left-handed user.]; and

a verification system for operably communicating with the electronic system, the verification system comprising a user storage, an authorization profile storage, and an audit log storage, the audit log storage being configured to store user identification information from said biometric sensor in response to an unsuccessful transaction attempt and denial of access with said electronic system.

2. (Amended) A pointing device as recited in claim 1, wherein the biometric sensor comprises a fingerprint sensor [for conveying information associated with the user's identity to the computer system].

7. (Amended) A pointing device as recited in claim [6] 1, wherein said biometric sensor is configured to convey [the attributes of the user's fingerprint comprises] a digitized scanned image of the user's fingerprint to said electronic system.

8. (Amended) A pointing device as recited in claim [6] 1, wherein said biometric sensor is configured to convey [the attributes of the user's fingerprint comprises] a compressed digital representation of the user's fingerprint to said electronic system.

9. (Amended) A pointing device as recited in claim [6] 1, wherein said biometric sensor is configured to convey [the attributes of the user's fingerprint comprises] a digital representation of a minutia of the user's fingerprint to said electronic system.

18. (Amended) A pointing device as recited in claim [16] 1, wherein the position sensor comprises a trackball that is movably-connected to the pointing device so that the trackball is [to be] positionable to either side of the [fingerprint sensor] biometric sensor so that the pointing device is equally well suitable for use by either a right-handed or a left-handed user.

Please add the following new claims:

-- 49. A pointing device as recited in claim 1, wherein the user storage, the authorization profile storage, and the audit log storage comprise one or more memory devices.

50. The pointing device of claim 49, wherein the one or more memory devices comprise a CD-ROM, a magnetic disk, an optical disk, or a flash memory.

51. The pointing device of claim 1, wherein the user storage, the authorization profile storage, or the audit log storage comprise a removable memory device.

52. The pointing device of claim 1, wherein the user storage, the authorization profile storage, or the audit log storage store encoded information.

53. The pointing device of claim 1, wherein the authorization profile storage stores permissible dates, times, functions, transactions, or any combination thereof associated with a user of said electronic system.

54. The pointing device of claim 1, wherein the audit log storage stores transaction information for a user who successfully accessed said electronic system.

55. The pointing device of claim 1, wherein the audit log storage stores a record of successful and unsuccessful system accesses to said electronic system.

56. The pointing device of claim 1, further comprising a substance detection sensor in operative relation with the biometric sensor.

57. The pointing device of claim 56, wherein the substance detection sensor detects narcotics, blood alcohol content, or any combination thereof of the user.

58. The pointing device of claim 57, wherein the verification system is configured to authorize or prevent access to the electronic system according to the user's blood alcohol content.

59. The pointing device of claim 56, wherein at least a portion of the substance detection sensor overlaps the biometric sensor.

60. The pointing device of claim 1, further comprising one or more additional biometric sensors in operative relation with the user and coupled to said interface.

61. A pointing device comprising:

an interface for operably communicating with an electronic system;

a position sensor, responsive to user movement thereof, for conveying positional information by way of said interface to the electronic system;

a user-depressable button for conveying selection information by way of said interface to the electronic system; and

a biometric sensor disposed at a location such that when operating said pointing device in a normal manner a user's foot rests naturally in a position to place a toe of the user's foot in proximity to and readable by said biometric sensor; and

a verification system for operably communicating with the electronic system, the verification system comprising a user storage, an authorization profile storage, and an audit log storage, the audit log storage being configured to store user identification information from said biometric sensor in response to an unsuccessful transaction attempt and denial of access with said electronic system.

62. A pointing device comprising:

a base;

a trackball mounted upon the base; and

an upper section having a left and a right side, said upper section moveably connected to the base such that the trackball is positionable adjacent said left or said right side, said upper section including at least one button formed substantially on a top surface of the upper section.

63. A pointing device as in claim 62 wherein:

the base is substantially circular in shape when viewed from above, thus having a generally circular perimeter; and

the trackball is mounted off-center on the base at a location intersecting the generally circular perimeter.

64. A pointing device as in claim 62 wherein the upper section is rotatably-connected to the base.

65. A pointing device as in claim 62 wherein the upper section comprises one or more buttons.

66. A pointing device as in claim 65 wherein:

when the upper section is rotated such that the trackball is located adjacent the left side, a right-handed user's hand, when operating the device in a normal manner, rests naturally in a position to place a finger of the user's right hand in proximity to one or more of the buttons and the user's right thumb in a position to move the trackball; and

when the upper section is rotated such that the trackball is located adjacent the right side, a left-handed user's hand, when operating the device in a normal manner, rests naturally in a position to place a finger of the user's left hand in proximity to one or more of the buttons and the user's left thumb in a position to move the trackball.

67. A computer verification system for use with a biometric sensor, said verification system comprising:

a processor coupled to the biometric sensor; and

a memory coupled to the processor, the memory comprising:

a user storage and an authorization profile being configured to verify an identification of a user each time the user inputs a request to an electronic system; and

an audit log storage being configured to store user identification information from the biometric sensor in response to an unsuccessful transaction attempt and denial of access with the electronic system.

68. The verification system of claim 67, wherein the memory comprises a CD-ROM, a magnetic disk, an optical disk, or a flash memory.

69. The verification system of claim 67, wherein the memory comprises a removable memory device.

70. The verification system of claim 67, wherein the memory stores encoded information.

71. A method for verifying a user of an electronic system coupled to a biometric sensor, the method comprising:

obtaining user identification information of the user with the biometric sensor;

obtaining a selection of the user for the electronic system;

comparing the user identification information with information stored in a user storage;

comparing the selection with authorization information stored in an authorization profile;

determining if the user is authorized to perform the selection; and

storing identification information and attempted transaction information of the user in the audit log storage if the user is not authorized to perform the selection and is denied access to the electronic system.

72. The method of claim 71, wherein the authorization information comprises permissible dates, times, functions, transactions, or any combination thereof associated with the user.

73. The method of claim 71, wherein storing identification information or storing transaction information comprises storing encoded information.

74. The method of claim 71, wherein the authorization information stored in the authorization profile is stored by one or more persons other than the user.

75. The method of claim 71, further comprising detecting a substance of the user with a substance detection sensor to determine if the user is authorized to access the electronic system.

76. The method of claim 75, wherein the substance comprises a narcotic or alcohol.

77. The method of claim 71, further comprising detecting a substance of the user with a substance detection sensor to determine if the user is authorized to perform the selection.

78. The method of claim 77, wherein the substance comprises a narcotic or alcohol. --

79. A verification system for operably communicating with an electronic system, the verification system comprising a user storage, an authorization profile storage, and an audit log storage, the audit log storage being configured to store information in response to a successful transaction attempt and grant of access with said electronic system and to an unsuccessful transaction attempt and denial of access with said electronic system.

80. The verification system of claim 79, wherein the information comprises digital information.

81. The verification system of claim 79, wherein the information comprises encoded information.

REMARKS

A. Status of the Claims

Claims 3-6 and 25-48 have been canceled without prejudice or disclaimer. Claims 1, 2, 7-9, and 18 have been amended. Claims 49-81 have been added. No new matter has been added.

B. Section 103 Rejections – Matchett and Lemelson

In the Office Action mailed February 29, 2000, the Examiner maintained rejections for certain pending claims while lodging new rejections based upon Matchett and Lemelson (U.S. Patent No. 5,202,929). The Office argued that Lemelson taught the features of Applicant's "verification system," recited in at least claim 1 and that a combination with Matchett would render the subject matter of the claims obvious. Applicant respectfully traverses.

1. Authorization Profile Storage

Claim 1 recites, in part, "a verification system . . . comprising a user storage, an authorization profile storage, and an audit log storage . . . ." As discussed in the specification, certain embodiments using such an authorization profile storage are afforded significant advantages:

> Additionally, information is stored into authorization profile storage 222, preferably by one who controls access to the system, such as a system administrator, a hotel cashier, or others, to specify which user may perform which transactions at what times and dates, etc. Thereafter, when a user attempts to access the system, his or her fingerprint is read by device 203, and compared with the known user storage 226, and the authorization profile storage 222 to determine whether to allow the particular user to perform the function requested. If so, the processor 216 then drives the access control signal 220, and logs the particular transaction, time, date, and identification information for the user. The identification of the user is verified continuously as long as the user is in contact with the biometric input device 203 .... *[I]f the user identifying information from the biometric device is matched with the user found in the known user storage 226, but the authorization profile storage 222 indicates that the particular user has requested something for which he or she is not authorized, then access is also denied*, and an audit log entry is also created in the audit log storage 224. This entry may include time, date, attempted transaction, and an indication of the user's identity, such as a name, a photographic image, or others." *Specification*, pages 15 through 16 (emphasis added).

Lemelson does not teach or suggest the features of independent Claim 1. Lemelson, in contrast to the present application, does not disclose, teach, or suggest a system utilizing an authorization profile storage as recited in the claims and explained, in relation to a specific embodiment, in the specification quoted above. In particular, the disclosure of Lemelson does not even mention (let alone teach or suggest) an authorization profile storage that allows for the storage of authorization information such as permissible dates, times, functions, or transactions for each user already known to a computer system. Further, Lemelson does not teach or suggest that such an authorization profile storage may be used to indicate whether a particular user has requested something (*e.g.*, by clicking a mouse) for which he or she is not authorized, and then to deny access to that user, if authorization does not exist.

Rather, Lemelson discloses a system in which a code signal or signals are generated that are used to identify a person entering and receiving data from a computer, which code signal is recorded for record purposes along with the information indicative of the information entered and/or received from the computer. *See* Abstract. Nowhere in Lemelson is there mention of an authorization profile storage as recited in the claims and explained above.

Because the cited art, taken alone or in any combination, does not teach or suggest the recited features of claim 1, and in particular, the features relating to an authorization profile storage, applicant respectfully submits that claim 1 is in condition for allowance. For at least the same reasons, all claims depending from claim1 are believed to be allowable as well, and Applicant therefore requests that those claims be allowed to pass to issue.

2. Audit Log Storage

Claim 1 recites, in part, "a verification system ... comprising a user storage, an authorization profile storage, and an audit log storage, *the audit log storage being configured to store user identification information from said biometric sensor in response to an unsuccessful transaction attempt and denial of access with said electronic system.*" As discussed in the specification, certain embodiments using such a verification system are afforded significant capabilities to detect internal fraud and unauthorized use:

> *If, at any time, a biometric reading is taken which does not match any user having a profile stored in the known user storage 226, access is denied and an audit log may be stored within the audit log storage 224 to provide a record of unsuccessful access attempts.* Such an audit log entry may include time, date, attempted transaction, *and a copy of the user identification information determined by the biometric device,* such as a scanned fingerprint image, a fingerprint minutia representation, or others. ... *Such an audit log affords a significant capability to detect internal fraud and other unauthorized use by persons known to the system, and indeed authorized perform some tasks, but not authorized for the task or function at the attempted time or date. Specification,* page 15 line 24 through page 16, line 10 (emphasis added).

Lemelson does not teach or suggest the features of independent claim 1. Lemelson, in contrast, discloses a system in which a code signal or signals are generated that are used to identify a person *entering and receiving data from a computer*, which code signal is recorded for record purposes along with the information indicative of the information *entered and/or received* from the computer. *See* Abstract. Thus, Lemelson allows for the storage of (a) a code signal to identify a person who has already gained access to the system, along with (b) information indicative of the information entered and/or received by that person who has already accessed the system. Although such a system may be useful to attribute data-entry errors to a person or person authorized to use, for instance, a cash register [*See* col. 11, lines 31-59], the system of Lemelson does not teach or suggest a system that allows for the storage of user identification information in response to an unsuccessful transaction attempt and denial of access with an electronic system, as recited in claim 1. In particular, there is no teaching in Lemelson to suggest that user identification information should be stored even if access is denied to a potential user in response to an unsuccessful transaction attempt.

At column 11, lines 31-59, Lemelson discloses that errors may be attributed to a person using a cash register because a code identifying the person is recorded with each cash-register transaction. Thus, if a user of the cash register performs an erroneous transaction, one may later attribute the error to the particular cash-register user. Again, as stated in the Abstract and confirmed by this cash-register example, the Lemelson system relates to the storage of information to identify a person who has already been allowed to enter and/or receive information from a computer (or cash register). The device recited in claim 1, however, provides even greater security measures because it is equipped with an authorization profile storage and an audit log storage that allow for the storage of user identification information in response to an *unsuccessful transaction attempt and denial of access* with an electronic system. In contrast to the system of Lemelson, Applicant's system therefore allows for (a) the denial of access if a transaction is not authorized and (b) the storage of user identification information in response to the unsuccessful transaction attempt and denial of access. So, if a cash-register were utilizing the recited features of claim 1, a cash-register user could be denied access (via the authorization profile storage) if he even attempted to enter an erroneous transaction – also, if he attempted such

a transaction, his user identification information (such as a fingerprint) could be stored in an audit log storage (even though he was denied access) so as to form a record of the unsuccessful transaction attempt. Thus, in contrast to the Lemelson system, certain cash-register errors could be prevented altogether (via a denial of access), and those even *attempting* to enter an erroneous transaction could be "finger-printed." Unlike the system of Lemelson, which allows a person to review and attribute erroneous transactions to a certain user *after they have already been completed and the damage is done*, the features of Applicant's invention both prevent and track fraud. These features, which are nowhere taught or even suggested by the cited art, act as a powerful fraud-deterrent for a variety of electronic systems

Because the cited art, taken alone or in any combination, does not teach or suggest the recited features of claim 1, and in particular, the features relating to an audit log storage being configured to store user identification information in response to an unsuccessful transaction attempt and denial of access with an electronic system, Applicant respectfully submits that claim 1 is in condition for allowance. For at least the same reasons, all claims depending from claim 1 are believed to be allowable as well, and Applicant therefore requests that those claims be allowed to pass to issue.

C. New Claims 49-60

New claims 49-60 are allowable for at least the reasons their parent claim 1 is allowable. Further, claims 56-59, relating to a substance detection sensor, are patentably distinct over the cited art as well – including Matchett, Lemelson, and Axelrod. Matchett, taken alone or in combination with Lemelson and Axelrod, does not teach or suggest the recited substance detection sensor. Matchett makes no mention of such a sensor, and the earlier-cited portions of Axelrod simply disclose that an auxiliary data input may include a breathalyzer so that additional data may be appended to a record. This does not amount to a teaching or suggestion of the features recited Applicant's claims, and for this reason as well, claims 56-59 are believed to be in condition for allowance.

D. New Claim 61

New independent claim 61, directed to a pointing device wherein the toe of a user's foot is in proximity to and readable by a biometric sensor, is believed to be in condition for allowance for at least the reasons claim 1 is allowable, as discussed in detail above.

E. New Claims 62-66

New claims 62-66 relate to a pointing device including a upper section moveably connected to a base such that a trackball is positionable adjacent a left or right side. These claims are believed to be allowable because such features are nowhere taught or suggested in the cited art, taken alone or in combination. Further, these claims are believed to be allowable for at least the reasons claim 25 of the parent-application to this application was deemed allowable by the Office.

F. New Claims 67-70

New claims 67-70 relate to a computer verification system including an audit log storage being configured to store user identification information from a biometric sensor in response to an unsuccessful transaction attempt and denial of access with an electronic system. These claims are in condition for allowance for at least the reasons claim 1 is allowable, as discussed in detail above.

G. New Claims 71-78

New claims 71-78 relate to a method for verifying a user of an electronic system and include the step of storing identification information and attempted transaction information of a user in an audit log storage if the user is not authorized to perform a selection and is denied access to the electronic system. These claims are allowable for at least the reasons claim 1 is allowable, as discussed in detail above. Further, claims 75-78, relating to a substance detection

sensor, are allowable because the features recited therein are not taught or suggested by the cited art, taken alone or in combination.

H. New Claims 79-81

New claims 79-81 relate to a verification system and is allowable for at least the reasons as discussed in detail above. In particular, none of the cited art, taken alone or in combination, teaches or suggests the recited user storage, authorization profile storage, and audit log storage.

CONCLUSION

Applicant believes that the foregoing remarks fully respond to all outstanding matters for this application. Applicant respectfully submits that the rejection of all the claims should be withdrawn, and that the claims should be passed to issue

Should the Examiner desire to sustain any of the rejections discussed in relation to this preliminary amendment, the courtesy of a telephonic conference between the Examiner and the undersigned attorney at 512-418-3018 is respectfully requested.

Respectfully submitted,

Michael C. Barrett

Michael C. Barrett
Reg. No. 44,523
Attorney for Applicant

FULBRIGHT & JAWORSKI L.L.P.
600 Congress Avenue, Suite 1900
Austin, Texas 78701
(512) 418-3000

Date: May 30, 2000

"Express Mail" mailing label number:

EM091692683US

POINTING DEVICE WITH BIOMETRIC SENSOR

David J. Kinsella

CROSS-REFERENCE TO RELATED APPLICATION

This application claims the benefit under 35 U.S.C. § 119(e) of U. S. Provisional Application Serial No. 60/027,254 filed September 30, 1996, entitled "Controller Device" and naming David J. Kinsella as inventor, which provisional application discloses an exemplary embodiment of the present invention, and which provisional application is incorporated herein by reference in its entirety.

BACKGROUND OF THE INVENTION

Field of the Invention

This invention is related to pointing devices, and more particularly to such devices providing biometric feedback to an attached electronic system.

Description of Related Art

Modern society demands that people may be identified for many reasons. These include limiting access to bank accounts, limiting access to certain facilities such as a security area, a computer room, a police department, or a military facility, limiting which people are authorized to pick up a child from a day care center, limiting access to government welfare checks and health benefits, determining which prisoner to parole, and limiting access to adult activities such as electronic gambling. This has led to increasing use of identification cards, passwords, and PIN numbers to supplement, in those instances where automated identification is either necessary or desirable, those situations where human recognition is either unavailable or will not suffice. This obviously results in an increasing array and assortment of various cards, passwords, and PIN numbers that active participants in today's increasingly electronic

society must carry with them (or ideally must memorize) to be able to access the functions and capabilities requiring such identification and verification.

Biometrics is the study of biological phenomena, and in the area of personal identification, some chosen characteristic of a person is used to identify or verify that person's identity. Biometric identification has gained interest in recent years because certain personal characteristics have been found to be substantially unique to each person and difficult to reproduce by an impostor. Further, the recording and analysis of biometric data is generally susceptible to automation owing to the increased use of computer controlled electronics and digital recording techniques. Biometric systems are automated methods of verifying or recognizing the identity of a living person on the basis of some physiological characteristic like a fingerprint or iris pattern, or some aspect of behavior like handwriting or keystroke patterns.

The biometric identifying characteristic may be biologically determined as with a fingerprint, or it may be some characteristic that is learned or acquired, such as handwriting or voice patterns. Ideally, the characteristic should be unique for every person and unvarying over the time frame during which the person may be tested for identification. The characteristic should also be difficult to duplicate by an impostor in order to secure against erroneous identification.

Some of the biometric characteristics most investigated today for use in a personal identification system include fingerprints, hand or palm prints, retina scans, signatures and voice patterns. Hand or palm print techniques typically evaluate the shape of a person's hand or other significant features such as creases in the palm, but these techniques may be fooled by templates or models of the hand of an authorized person. Retina scanning techniques evaluate the pattern of blood vessels in a person's retina. A drawback of this technique is that the blood vessel pattern may vary over time, e.g., when alcohol is in the blood stream or during irregular use of glasses or contact lenses. Also, a user may feel uneasy about having his or her eye illuminated for retina scanning or the possibility of eye contamination if there is contact between the eye and the scanning apparatus. Signatures can be forged easily and must usually be evaluated by a human operator, although work has been done on automated

systems that evaluate the dynamics of a person's handwriting, such as the speed and the force of hand movement, pauses in writing, etc. Using voice patterns as the identifying characteristic encounters difficulties owing to the wide variations in a person's voice over time, the presence of background noise during an evaluation and the potential for an impostor to fool the system with a recording of the voice of an authorized person.

The most commonly used biometric characteristic and the one that has been the most investigated and developed is, of course, the fingerprint. Up until now, the technology of personal identification through fingerprint analysis has been used mainly in law enforcement, and this long term experience with fingerprint analysis has developed a large amount of information about fingerprints and has confirmed the uniqueness of a person's fingerprints. Historically, in law enforcement, fingerprints have been recorded by inking the fingerprint and making a print on a card for storage.

A fingerprint identification system is described in an article entitled "Vital Signs of Identity" by Benjamin Miller (IEEE Spectrum, February 1994, pp. 22-30). The system for recognizing fingerprints requires the user to press a finger onto a glass or Plexiglas platen. Image sensors under the platen and a charge-coupled device (CCD) array capture the fingerprint image. A custom computer system and software analyses the digitized image and converts it to an approximately 1K mathematical characterization which is compared against data stored in the local terminal or in networked versions of the system in a remote personal computer.

Rather than requiring a user to explicitly engage with verification devices, transparent verification attempts to identify the identity of a user not only unobtrusively, but during a transaction and using normal user interactions with the system. For example, a voice recognition system which also is able to identify a user by his voice pattern provides a capability of identifying a user as the user is speaking a request or command to the system, rather than as an explicit identification action or request by the user.

U.S. Patent No. 5,229,764 to Matchett et al. describes a continuous biometric authentication matrix. This system activates and analyzes the biometric data from a plurality of biometrically-oriented personal identification devices at intermittent intervals and selectively allows or prevents continued use of a particular protected system or device by a particular individual. The system acts as a continuously functioning gate between a system to be protected and a prospective user. Many of the biometrically-oriented personal identification devices in the Matchett system attempt some degree of transparent verification and include thumbscan, digital photo, voice prints, fingerprints and others. One such device is a joystick device shown in Figure 7 incorporating a thumbscan sensor on the top end of the joystick. In Figure 8A a computer mouse is depicted carrying a hand geometry reader in a mouse casing. The hand geometry reader is wired through the mouse and its leads run back to the rest of the scanning unit along the same conduit PG as that of the mouse. Figure 8B depicts a mouse having a thumbscan unit sensor incorporated into its side. The thumbscan sensor may be oriented relative to a mouse casing adapting it either for right-handed persons or left-handed persons or both. A mouse lead is modified or replaced to carry both the mouse data and the sensor data.

A pointing device such as a computer mouse, joystick, or trackball, includes two principal components: a positional indicator allows movement by a user to be communicated as user positional information to an attached system (e.g., a computer system) to allow, for example, a pointer to be moved around a window or a screen of a graphical user interface; and input switches or buttons so that a user can provide selection information to the system which corresponds to a particular location to which the positional indicator has been moved. Both kinds of information are communicated through a typically small cable to the system to which the pointing device is attached. Alternatively, infrared beams and RF interfaces have also been used to allow for wireless pointing devices, particularly a wireless mouse.

Notwithstanding these devices, there is a need for additional and improved verification devices and capabilities for electronic systems, particularly those

verification devices that provide for transparent continuous verification during normal user interactions with the system.

SUMMARY OF THE INVENTION

The present invention includes a pointing device which incorporates a biometric sensor at a location such that when operating the pointing device in a normal manner, a user's hand rests naturally in a position to place a finger of the user's hand in proximity to and readable by the biometric sensor. The location of the biometric sensor is equally well suitable for use by either a right-handed or a left-handed user, irrespective of hand size. Along with positional information from a position sensor and user selection information from at least one user-depressable button, the pointing device of the present invention also conveys to an attached system information associated with the user's identity detected by the biometric sensor. In one embodiment, the biometric sensor is a fingerprint sensor. Such a pointing device is well suited to both transparent verification as well as continuous, real-time verification, for if a user removes his or her hand from the natural position when using the device, the user's fingerprint will no longer be detectable by the fingerprint sensor, and the attached electronic system can be alerted as to the need to re-authenticate any additional attempts at using the pointing device. Minimal technical knowledge is required, for the identification functions are incorporated into a familiar pointing device. It affords a virtually foolproof, easily-used, and immediate method of identifying a user desiring access. A system audit log which records all attempted transactions, both authorized as well as non-authorized, may be easily implemented.

In one embodiment of the present invention, a pointing device includes an interface for operably communicating with an electronic system, a position sensor, responsive to user movement thereof, for conveying user positional information by way of said interface to the electronic system, a user-depressable button for conveying user selection information by way of said interface to the electronic system, and a biometric sensor disposed at a location such that when operating said pointing device in a normal manner a user's hand rests naturally in a position to place a finger of the

user's hand in proximity to and readable by said biometric sensor, said location equally well suitable for use by either a right-handed or a left-handed user.

In another embodiment of the present invention, a pointing device includes an interface for operably communicating with a computer system, a base, a trackball mounted upon the base, an upper section connected to the base and including at least one button formed substantially on a top surface of the upper section, and a fingerprint sensor mounted within the upper section and disposed at a location such that when operating said pointing device in a normal manner, a user's hand rests naturally in a position to place a finger of the user's hand in proximity to and readable by said fingerprint sensor.

In yet another embodiment of the present invention, a pointing device includes an interface for operably communicating with a computer system, a base which is substantially circular in shape when viewed from above, thus having a generally circular perimeter, a trackball mounted off-center on the base at a location along the generally circular perimeter, an upper section connected to the base and including at least one button formed substantially on a top surface of the upper section, and a fingerprint sensor mounted within the upper section and disposed at a location such that when operating said pointing device in a normal manner a user's hand rests naturally in a position to place a finger of the user's hand in proximity to and readable by said fingerprint sensor.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention may be better understood, and its numerous objects, features, and advantages made apparent to those skilled in the art by referencing the accompanying drawings.

Figures 1, 2 and 3 are a top view, a side view, and a rear view, respectively, of one embodiment of a computer pointing device in accordance with the present invention.

Figure 4 is a cross-sectional view of the embodiment shown in Figure 1.

Figure 5 is an electrical block diagram of an embodiment of electronic circuitry useful within the computer pointing device shown in Figure 1.

Figure 6 is an electronic schematic drawing of interface circuitry depicted in Figure 5.

Figure 7 is an electronic schematic drawing of user-button circuitry depicted in Figure 5.

Figure 8 is an electronic schematic drawing of video circuitry depicted in Figure 5.

Figure 9 is a block diagram of a system incorporating the computer pointing device shown in Figure 1.

The use of the same reference symbols in different drawings indicates similar or identical items.

DESCRIPTION OF THE PREFERRED EMBODIMENT(S)

Trackball Embodiments

Figure 1, Figure 2, and Figure 3 illustrate a top view, a side view, and a rear view, respectively, of a trackball embodiment of the present invention. Referring specifically to Figure 1, a computer trackball pointing device 10 includes a base 12 which is substantially circular in shape and has a generally circular perimeter 14. It is preferably approximately 6 inches in diameter, weighs approximately 2 pounds, and is constructed generally of heavy duty plastic, although other dimensions are plausible. A chamfered surface 25 is formed between the top surface of base 12 and the perimeter surface 14. A trackball 16 is mounted off-center on the base 12 within a housing 28 formed on the base at a location intersecting the generally-circular perimeter surface 14. An upper section 18 is connected to the base 12 and includes, for this embodiment, three user-depressable buttons 22A, 22B and 22C formed substantially on a top surface 24 of the upper section 18. An interface 20 connects between the computer trackball pointing device 10 and an attached computer system,

or other electronic system. A fingerprint sensor (not shown) or other suitable biometric sensor is mounted, for this embodiment, below the center button 22B within the upper section 18 which is a location such that when operating the trackball pointing device 10 in a normal manner, a user's hand rests naturally in a position to place the second finger of the user's hand (i.e., the "middle" finger) in proximity and readable by the fingerprint sensor located below user depressable button 22B. The arrangement is well suited for all users regardless of hand size. The trackball pointing device 10 is adaptable for both right-handed and left-handed users because the upper section 18 is rotatably connected to the base 12 so that the trackball is positionable to either a position leftward or a position rightward of the upper section. The axis of this rotation is indicated at location 27 and provides for a symmetrical positioning of trackball 16 on either the left side or the right side of upper section 18.

Referring now to Figure 2, the bottom surface 30 of the base 12 is substantially flat and may include cushioning pads (not shown) such as low-profile self-adhesive rubber feet, or some other non-scratching surface treatment. The top surface 24 of the upper section 18 is shown, for this embodiment, as a substantially uniformly curved, convex surface which provides a comfortable surface for a user's palm and lower finger regions to rest comfortably upon the computer trackball pointing device 10. Referring specifically to the read view shown in Figure 3, the interface 20 is shown as a cabled interface passing through the rear surface of the upper section 18. The flat bottom surface 30 of base 12, particularly when implemented with a reasonable large diameter, allows the computer trackball pointing device 10 to easily be placed on a user's lap, or on a soft surface such as a bed, rather than requiring a hard surface such as a desktop.

To rotate the position of the trackball 16 from one side to the other, the computer trackball pointing device 10 is elevated from the surface upon which it rests, the upper section 18 is maintained in a direction pointing away from the user (the interface 20 pointing away from the user) and the base 12 is rotated upon axis 27 sufficiently to cause the trackball 16 within housing 28 to be moved from, for

example, the left side of the upper section 18 (as is indicated in Figure 1) to the right side of upper section 18.

Details of the rotating connection which provides this capability as well as other internal details of the trackball pointing device 10 are shown in cross-section in Figure 4. Center column 54 is formed as part of the upper section 18 and provides the axis point for the base 12 to rotate with respect to the upper section. Screw 42 (and optionally a washer, not shown) fasten the upper section 18 to the base 12, as well as provide the axis of rotation for the base 12. Interface 20 is now more clearly illustrated as being connected to the upper section 18 so that when used by either right-handed or left-handed users, and when the three buttons are positioned away from the user (i.e., in a rearward direction), the interface is held and pointed in the same direction even as the base is rotated either leftward or rightward of the upper section. Lower circuit board 40 is shown providing a suitable carrier for necessary electronics to implement the functionality required of the computer trackball pointing device 10. For example, integrated circuit 52 is shown attached to a lower printed wiring board 40 (PWB), and an upper PWB-41 is shown electrically interconnected by interface cable 50 to the lower PWB-40. The upper PWB-41 includes a depressable switch 48 and a fingerprint sensor 44. In this embodiment, user depressable switch 22B is formed of a transparent material through which the fingerprint sensor (which may be an optical CCD sensor) may view the fingerprint of a user whose finger rests upon the surface of transparent button 22B. When depressed by a user, the button 22B causes switch 48 to be depressed by linkage 46. This allows the center button 22B to be an operable button, able to sense when a user depresses the button and to communicate such information to an attached electronic system. But the computer trackball pointing device 10 also provides, by way of the fingerprint sensor 44 viewing the fingerprint of the user through the transparent material forming button 22B, and at the same time, a scan of the user's fingerprint. This affords the capability of identifying or authorizing the particular user. When connected to an attached electronic system, this trackball pointing device 10 provides for the ability to read the fingerprint of a user, even as the user is using that very finger to make input selections to the attached electronic system.

It should also be appreciated when looking at the computer input trackball device depicted in Figures 1 through 4 that when the upper section 18 is rotated such that the trackball 16 is located leftward of the upper section 18, a right-handed user's hand when operating the device in a normal manner rests naturally in a position to place the second finger of the user's right hand in proximity and readable by the fingerprint sensor 44 and the user's right thumb in a position to comfortably move the trackball 16. Moreover when the upper section 18 is rotated such that trackball 16 is located rightward of the upper section 18, a left-handed user's hand when operating the device in a normal manner rests naturally in a position to place the second finger of the user's left hand in proximity to and readable by the fingerprint sensor 44 and the user's left thumb in a position to comfortably move the trackball 16.

Generally speaking, the fingerprint sensor 44 conveys information associated with the user's identity to the computer system attached by way of interface 20. This information may include a signal indicating whether the user is authorized to access the computer system. For example, a storage means such as an electronic memory may be included within the trackball pointing device 10 for storing information associated with the identity of at least one authorized user which is received from the attached computer system. Thereafter the fingerprint sensor 44 utilizing such storage, within the trackball pointing device 10, of authorized users may independently make a determination that a particular user attempting to use the device is an authorized user upon comparison of actual measured fingerprint with stored information from the authorized list. In other instances the information associated with the user's identity may include a signal indicating the attributes of the user's fingerprint so that the attached computer or other electronic system may determine whether the user is authorized to access the computer system. Examples of such attributes of the user's fingerprint include a digitized scanned image of the user's fingerprint, compressed representations of the user's fingerprint in digital or other form including a digital representation of the minutia of the user's fingerprint.

Other embodiments of similar input devices incorporating a biometric sensor may include a variety of different button positions in which the fingerprint sensor or

other biometric sensor is located below a particular one of the button positions. Figure 1 shows an pointing device 10 having three button positions, each of which is depicted to illustrate an operable button (e.g., buttons 22A, 22B, and 22C) at each of the button positions, but a particular button position may have either an inoperable button at such a location or no button whatsoever at the location. Moreover, the fingerprint sensor 44 or other biometric sensor may be located below a button position, whether operable or not, or at a location not beneath a button position. In another embodiment a three-button mouse includes a fingerprint sensor 44 disposed beneath an operable or inoperable center button position as is similarly depicted within the upper section 18 of the computer trackball pointing device 10 shown in Figure 1.

While the base of the computer trackball pointing device 10 is shown in Figure 1 as being rotatably connected to the upper section 18, other variations are equally plausible. For instance, a fixed connection could be easily implemented as a single-piece construction and could be configured for a right-handed or a left-handed user rather than as a single device which provides equal suitability to either a right-handed or a left-handed user. Likewise, similar moveable connections rather than a rotational connection are also contemplated which would allow a trackball device to be positioned in at least one of two locations such that suitable use for both right-handed and left-handed users may be achieved. The interface 20 which is depicted in Figure 1 as being a wired interface may also be implemented as a wireless interface and could include an infrared, a radio frequency or any variety of other wireless techniques. The interface may instead include a wireless interface having a transducer located at a rear surface of the upper section 18. Fingerprint sensor 44 may be implemented as an optical imaging array as depicted in Figure 4 in which the user's fingerprint is imaged through a transparent material forming button 22B. Such optical imaging arrays are commercially available, including from Suni Imaging Systems, Mountain View, California, and from Keytronics, Washington, D.C. Alternatively such a fingerprint sensor 44 may also be implemented as a capacitive imaging array, such as the FingerLoc™ series of sensors, available from the Harris Corporation, Melborne, Florida.

Figure 5 is an electrical block diagram of one embodiment of an electronic sub-system 50 which may be implemented within the computer trackball pointing device 10 shown in Figure 1. The sub-system 50 includes an interface 51 which communicates to an attached computer system or other electronic system, a controller 55 for general control functions and for implementing traditional computer "mouse" functions, a button block 52 which includes traditional computer mouse user-depressable buttons, a pointer 53 which, in this case, includes circuits for implementing a computer trackball pointing device, and CCD camera 54 which provides a capability of visually scanning a user's fingerprint.

The interface 51 includes a group 60 of wires which provides communication to and from an attached system. These wires are preferably implemented using an unshielded twisted pair (UTP) cable having three twisted pairs of wires for connecting, using suitable connectors, to an attached computer or other electronic system. The group 60 of wires includes power terminal RAW12 and ground terminal GROUND for receiving power and ground from the attached system, differential video signal lines VIDEO+ and VIDEO- for conveying a differential video signal to the attached system, and serial data lines DATA and DATA_RET for respectively conveying serial data to and from the attached system. In other embodiments, a wireless interface, such as an infrared or RF interface, may also be used. On-board batteries may used to power the pointing device in lieu of power cables.

The button block 52 includes three user-depressable buttons (not shown) and conveys a signal for each button (BUTTON1, BUTTON2, and BUTTON3) in a group 57 of wires to the controller 55. Other numbers of buttons are also possible, including one, or two. The pointer 53 includes the trackball position sensor and communicates positional information using signals X_CLK, X_DIR, Y_CLK, and Y_DIR to the controller 55 via the group 56 of wires. The pointer 53 may also include a computer mouse position sensor. Power is also received from the interface 51 via a wire within the group 56 of wires.

The controller 55 receives power from the interface 51 via one of the wires 56, and also sends and receives serial data to/from the interface 51 via wires 59 and 58,

respectively. Controller 55 provides for a point-and-click selection capability and data transfer capability to an attached system, to provide the traditional capabilities associated with a computer mouse or trackball.

Biometric sensor 54, such as a CCD camera, receives power from the interface 51 and conveys (for this example) a video signal to the interface 51 via wire 60. In other embodiments, other types of biometric sensors may be used, such as an capacitive fingerprint sensor rather than an optical sensor. One such sensor is the FingerLoc™ series of capacitive imaging array sensors, available from the Harris Corporation, Melborne, Florida. Additional control and data signals (not shown) between the interface 51, the controller 55, and the biometric sensor 54 are to be expected in other embodiments.

Referring now to Figure 6, one embodiment of the interface 51 includes a voltage regulator 70 for generating a +5 volt power supply from an incoming +12 volt supply, along with various related filtering capacitors and a ferrite bead. Twin video amplifiers 71, 72 produce a differential video signal from a single-ended signal received from the biometric sensor 54. Video amplifier 71 is configured as a unity gain amplifier with a 75 ohm output impedance, and video amplifier 72 is configured as a negative unity gain amplifier, also with a 75 ohm output impedance. Serial data buffers 73, 74 provide simple buffering to an already serial signal received from the controller 55 (e.g., HDATA_OUT) or received from the attached system (e.g., HDATA_IN).

Figure 7 depicts one embodiment of the button block 52. A respective pull-up resistor to a +5 power supply voltage is momentarily connected to ground by a respective user-depressable switch, and which generates the respective button signal.

Figure 8 illustrates one embodiment of a biometric sensor 54 incorporating a CCD camera system which may be implemented within a pointing device, such as within the computer trackball pointing device 10 shown in Figure 1.

System Embodiments

Figure 9 illustrates a system 200 which includes a user interface terminal 202 connected via a connection 210 to a computer verification system 212. User interface terminal 202 includes a biometric input device 203 (e.g., a computer trackball pointing device 10), a keyboard 206, a display 204, and an interface controller 208. The computer verification system 212 includes an interface controller 214, a processor 216, and memory 218. The processor 216 generates an access control signal 220 when user identification and/or authorization has been confirmed and access to a particular system or feature (not shown) is warranted. Such an access-controlled system may reside within the computer verification system 212, or may be external to the computer verification system 212, and may include access to physical equipment or electronically stored or transmitted information.

Memory 218 includes known user storage 226 for storing the identification information, such as a fingerprint "signature," of users already known to the system 212. Memory 218 also includes authorization profile storage 222 for storing authorization information (e.g., permissible dates / times / functions / transactions / machines) for each user already known to the system 212. Memory 218 also includes an audit log storage 224 for storing successful and unsuccessful system accesses, as well as transaction information for users who successfully gain access to the system. The authorization profile storage 222, audit log storage 224, and known user storage 226 may be implemented together as one or more digital memory devices, or may be implemented using separate memory technologies, such as writable CDROM, magnetic disk, optical disk, flash memory, and other well known technologies. Advantageously, one or more of the authorization profile storage 222, the audit log storage 224, and the known user storage 226 may store encoded information, and may be implemented as an electronic memory device connected to the system 212, such as a removable PC card memory device. This affords, for example, an authorized user to carry his profile in a removable device and allows gaining access to any system to which the removable device is connected.

A user initializes the verification system by first using the biometric input device 203, such as the computer trackball pointing device 10, to sense the biometric information (in this example, a fingerprint), to digitize it, optionally compress it or otherwise extract a "signature" representative of that user's fingerprint, and store the information, along with other user identifying information, into the known user storage 226. The stored "signature" is then used to identify and/or verify subsequent attempted accesses of the system 200.

Additionally, information is stored into authorization profile storage 222, preferably by one who controls access to the system, such as a system administrator, a hotel cashier, or others, to specify which user may perform which transactions at what times and dates, etc. Thereafter, when a user attempts to access the system, his or her fingerprint is read by device 203, and compared with the known user storage 226 and the authorization profile storage 222 to determine whether to allow the particular user to perform the function requested. If so, the processor 216 then drives the access control signal 220 and logs the particular transaction, time, date, and identification information for the user. The identification of the user is verified continuously as long as the user is in contact with the biometric input device 203 (for this example, the computer trackball pointing device 10). Each time the user inputs a system request, the verification process must be completed and maintained prior to continuing the use of the device being accessed. Verification times of several seconds are achievable with available processors and algorithms. If the use of the accessed device is discontinued, the verification process must be completed once prior to gaining access to the desired device, and use must be maintained for continued access.

If, at any time, a biometric reading is taken which does not match any user having a profile stored in the known user storage 226, access is denied and an audit log may be stored within the audit log storage 224 to provide a record of unsuccessful access attempts. Such an audit log entry may include time, date, attempted transaction, and a copy of the user identification information determined by the biometric device, such as a scanned fingerprint image, a fingerprint minutia representation, or others. Alternatively, if the user identifying information from the

biometric device is matched with a user found in the known user storage 226, but the authorization profile storage 222 indicates that the particular user has requested something for which he or she is not authorized, then access is also denied and an audit log entry is also created in the audit log storage 224. This entry may include time, date, attempted transaction, and an indication of the user's identity, such as a name, a photographic image, or others.

Such an audit log affords a significant capability to detect internal fraud and other unauthorized use by persons known to the system, and indeed authorized to perform some tasks, but not authorized for the task or function at the attempted time or date . For example, assume the system 200 is configured to provide access control to a cash register machine. Assume Sally and Mary are both registered employees known to the system and each has an entry in the known user storage 226. Further assume that Mary is continuously and properly verified during her shift as being authorized to engage in the type of transactions normally performed at her cash register. But if, during one of Mary's short work breaks, Sally tries to access the cash register during a time she is unauthorized, the system logs her unsuccessful attempt along with her name, picture, fingerprint, or some other identifying information. If Sally is unknown to the system altogether (i.e., no entry in the known user storage 226), then the audit log created may include, as well, as much identifying information, such as a fingerprint image, as possible to help law enforcement officials or others in identifying the person responsible for the unsuccessful access.

The computer trackball pointing device 10 may generate a scanned image of a users fingerprint, which is communicated to a host system for verification processing. Alternatively, the verification capability may reside within the computer trackball pointing device 10 along with authorized user keys to allow the pointing device to determine whether a user is authorized, without significant data transfers between the computer trackball pointing device 10 and the attached system. For example, the FingerLoc™ series of devices, available from the Harris Corporation of Melborne, Florida, includes a down-loadable local memory for storing fingerprint profiles for up to 100 users, and includes a processor for independently determining whether an

observed fingerprint matches one stored within the local memory, without intervention from an attached host processor. In such an embodiment, the computer trackball pointing device 10 may therefore include biometric identification software, as well.

Combined Identification/Substance Detection Embodiments

In some embodiments of a pointing device employing an optical scanning capability, such as a color CCD imager, it may be possible to determine the blood alcohol content of the user simultaneously with scanning the fingerprint to determine the identification of the user. Such a combined identification/sobriety sensor would only allow access to an authorized person if he/she was sober. This could have tremendously beneficial applications in security access to military bases, power plants, industrial machinery areas, employer liability concerns, and others. A sensitive patch material is commercially available which, when in contact with a person's skin, changes color in response to chemical variations in the user's perspiration, and which is correlated to the person's blood alcohol content. A small patch of such material, if placed over the transparent window, allows a user's finger to be partially visible (and the patch could be sized small enough to preserve enough fingerprint information) for identifying a person, and yet still be large enough to sense perspiration variations, and change color appropriately enough to determine the blood alcohol content of the user. Such an arrangement would make the combined identification/sobriety sensor difficult for two people to fool. If the "authorized" person was drunk, and another person, a "thief," was sober, the system would still be hard to defeat. Such a system may be hard enough to defeat to permit unattended sobriety/identification terminals, for remote access control which ensures a sober user, not just an authorized user. Materials which may be used to detect other substances than alcohol, such as cocaine or other narcotics, may also be available and incorporated advantageously as described above.

Ten Finger Identification With Single Sensor

A pointing device such as a computer trackball pointing device 10 as shown in Figure 1, or any other device which has only one fingerprint sensor, may be used with up to all ten fingers to decrease the statistical chance of authentication error. For example, a user during the initialization sequence may be requested to place each of his/her fingers on the single fingerprint sensor so the system may learn each of the user's ten fingerprints. Then, periodically or at random, frequent intervals, the user may be requested by the system to place a certain finger on the sensor before the system proceeds. Also, such a system may request all tens fingers be presented sequentially to the sensor after a predetermined period of inactivity. The system may also demand all ten fingers be sequentially placed upon the fingerprint sensor before granting initial access, or after a predetermined period of user inactivity.

Foot-Print Embodiment

Embodiments of the present invention may include adaptations which allow a foot-operated pointing device which identifies a user by matching foot prints. A position sensor may be implemented in a much larger size to be easily operable with one or both feet, while large user-depressable buttons may be engaged with one or more toes, during which time one or more sensors scans portions of the user's foot or feet.

Other Embodiments

It should be appreciated that a mouse position sensor may be used instead of a trackball position sensor by using the teachings of this disclosure.

A fingerprint sensor may also be placed below a transparent trackball to allow reading a user fingerprint through the trackball. Distortions caused by the curvature of the trackball may be accounted for by software transformations of scanned fingerprint image data, or by merely "teaching" the fingerprint of an authorized user by using the same distorted optics.

While the invention has been described with respect to the embodiments set forth above, the invention is not necessarily limited to these embodiments. For example, while recited using a typical context of use with a computer system, a computer pointing device may be attached to a wide variety of other electronic systems which are essentially computer systems or computer-controlled systems, such as set-top boxes for television, security systems, and others. Moreover, a pointing device as described herein is particularly well suited for use with a system along with other biometric sensors, such as a biometric retinal scanner which may be used for identification/authentication and/or substance detection, as well as with a removable PC card memory storage to store biometric information for the authorized user. Accordingly, other embodiments, variations, and improvements not described herein are not necessarily excluded from the scope of the invention, which is defined by the following claims.

a biometric sensor disposed at a location such that when operating said pointing device in a normal manner a user's hand rests naturally in a position to place a finger of the user's hand in proximity to and readable by said biometric sensor, said location equally well suitable for use by either a right-handed or a left-handed user, said biometric sensor for conveying user biometric information to the electronic system.

WHAT IS CLAIMED IS:

1. A pointing device comprising:

an interface for operably communicating with an electronic system;

a position sensor, responsive to user movement thereof, for conveying user positional information by way of said interface to the electronic system;

a user-depressable button for conveying user selection information by way of said interface to the electronic system; and

a biometric sensor disposed at a location such that when operating said pointing device in a normal manner a user's hand rests naturally in a position to place a finger of the user's hand in proximity to and readable by said biometric sensor, said location equally well suitable for use by either a right-handed or a left-handed user.

2. A pointing device as recited in claim 1 wherein the biometric sensor comprises a fingerprint sensor for conveying information associated with the user's identity to the computer system.

3. A pointing device as recited in claim 2 wherein the information associated with the user's identity comprises a signal indicating whether the user is authorized to access the computer system.

4. A pointing device as recited in claim 3 wherein the fingerprint sensor comprises storage means for storing information associated with the identity of at least one authorized user.

5. A pointing device as recited in claim 4 wherein information associated with the identity of at least one authorized user is operably received by the fingerprint sensor from the computer system for storage within the storage means.

6. A pointing device as recited in claim 1 wherein the information associated with the user's identity comprises a signal indicating attributes of the user's fingerprint, so that the computer system may determine whether the user is authorized to access the computer system.

7. A pointing device as recited in claim 6 wherein the attributes of the user's fingerprint comprises a digitized scanned image of the user's fingerprint.

8. A pointing device as recited in claim 6 wherein the attributes of the user's fingerprint comprises a compressed digital representation of the user's fingerprint.

9. A pointing device as recited in claim 6 wherein the attributes of the user's fingerprint comprises a digital representation of minutia of the user's fingerprint.

10. A pointing device as recited in claim 1 wherein the position sensor comprises a mouse.

11. A pointing device as recited in claim 2:
further comprising at least one button position; and
wherein the fingerprint sensor is disposed below a particular one of the at least one button positions.

12. A pointing device as recited in claim 11 wherein an operable button is located at the particular button position.

13. A pointing device as recited in claim 11 wherein an inoperable button is located at the particular button position.

14. A pointing device as recited in claim 11 wherein no button is located at the particular button position.

15. A pointing device as recited in claim 11 wherein:

the at least one button positions numbers three; and

the fingerprint sensor is disposed below a centermost button position of the three button positions.

16. A pointing device as recited in claim 1 wherein the position sensor comprises a trackball.

17. A pointing device as recited in claim 16 wherein the position sensor further includes a second trackball.

18. A pointing device as recited in claim 16 wherein the trackball is movably-connected to the pointing device to be positionable to either side of the fingerprint sensor.

19. A pointing device as recited in claim 18 wherein the trackball is rotatably-connected to the pointing device.

20. A pointing device as recited in claim 1 wherein the interface comprises a cabled interface.

21. A pointing device as recited in claim 1 wherein the interface comprises a wireless interface.

22. A pointing device as recited in claim 11 wherein:

the fingerprint sensor includes an optical imaging array; and

the particular button position includes a transparent material through which the user's fingerprint may be imaged by the imaging array.

23. A pointing device as recited in claim 11 wherein:

the fingerprint sensor includes a capacitive imaging array located at the particular button position contactable by the user's finger so that the user's fingerprint may be imaged by the capacitive imaging array.

24. A pointing device as recited in claim 23 wherein:

the fingerprint sensor is incorporated into an operable button located at the particular button position.

25. A pointing device comprising:

an interface for operably communicating with a computer system;

a base;

a trackball mounted upon the base;

an upper section connected to the base and including at least one button formed substantially on a top surface of the upper section; and

a fingerprint sensor mounted within the upper section and disposed at a location such that when operating said pointing device in a normal manner, a user's hand rests naturally in a position to place a finger of the user's hand in proximity to and readable by said fingerprint sensor.

26. A pointing device as in claim 25 wherein:

the base is substantially circular in shape when viewed from above, thus having a generally circular perimeter; and

the trackball is mounted off-center on the base at a location intersecting the generally circular perimeter;

27. A pointing device as in claim 25 wherein:

the upper section is movably-connected to the base such that the trackball is positionable to both a position leftward of and rightward of the upper section.

28. A pointing device as in claim 27 wherein the upper section is rotatably-connected to the base.

29. A pointing device as in claim 26 wherein the upper section is fixably-connected to the base.

30. A pointing device as in claim 25 wherein the upper section comprises:

a plurality of button positions formed substantially on a rearward portion of the top surface of the upper section; and

wherein the fingerprint sensor is located beneath a particular one of the button positions.

31. A pointing device as in claim 30 wherein an operable button of the pointing device is located at the particular button position.

32. A pointing device as in claim 30 wherein no operable button of the pointing device is located at the particular button position.

33. A pointing device as in claim 30 wherein an inoperable button of the pointing device is located at the particular button position.

34. A pointing device as in claim 25 wherein:

the interface includes a cable passing through a rear surface of the upper section.

35. A pointing device as in claim 25 wherein:

the interface includes a wireless interface having a transducer disposed at a rear surface of the upper section.

36. A pointing device as in claim 28 wherein:

when the upper section is rotated such that the trackball is located leftward of the upper section, a right-handed user's hand, when operating the

device in a normal manner, rests naturally in a position to place a finger of the user's right hand in proximity to and readable by the fingerprint sensor and the user's right thumb in a position to comfortably move the trackball; and

when the upper section is rotated such that the trackball is located rightward of the upper section, a left-handed user's hand, when operating the device in a normal manner, rests naturally in a position to place a finger of the user's left hand in proximity to and readable by the fingerprint sensor and the user's left thumb in a position to comfortably move the trackball.

37. A pointing device as recited in claim 30 wherein:

the fingerprint sensor includes an optical imaging array; and

the particular button position includes a transparent material through which the user's fingerprint may be imaged by the imaging array.

38. A pointing device as recited in claim 30 wherein:

the fingerprint sensor includes a capacitive imaging array located at the particular button position contactable by the user's finger so that the user's fingerprint may be imaged by the capacitive imaging array.

39. A pointing device as recited in claim 38 wherein:

the fingerprint sensor is incorporated into an operable button located at the particular button position.

40. A pointing device comprising:

an interface for operably communicating with a computer system;

a base which is substantially circular in shape when viewed from above, thus having a generally circular perimeter;

a trackball mounted off-center on the base at a location along the generally circular perimeter;

an upper section connected to the base and including at least one button formed substantially on a top surface of the upper section; and

a fingerprint sensor mounted within the upper section and disposed at a location such that when operating said pointing device in a normal manner a user's hand rests naturally in a position to place a finger of the user's hand in proximity to and readable by said fingerprint sensor.

41. A pointing device as in claim 40 wherein:

the upper section is rotatably-connected to the base such that the trackball is positionable to both a position leftward of and rightward of the upper section.

42. A pointing device as in claim 41 wherein the upper section comprises:

a plurality of button positions formed substantially on a rearward portion of the top surface of the upper section; and

wherein the fingerprint sensor is located beneath a particular one of the button positions.

43. A pointing device as in claim 42 wherein:

an operable button of the pointing device is located at the particular button position; and

the interface includes a cable passing through a rear surface of the upper section.

44. A pointing device as in claim 41 wherein:

when the upper section is rotated such that the trackball is located leftward of the upper section, a right-handed user's hand, when operating the device in a normal manner, rests naturally in a position to place a finger of the user's right hand in proximity to and readable by the fingerprint sensor and the user's right thumb in a position to comfortably move the trackball; and

when the upper section is rotated such that the trackball is located rightward of the upper section, a left-handed user's hand, when operating the device in a normal manner, rests naturally in a position to place a finger of the user's left hand in proximity to and readable by the fingerprint sensor and the user's left thumb in a position to comfortably move the trackball.

45. A pointing device as recited in claim 42 wherein:

the fingerprint sensor includes an optical imaging array; and

the particular button position includes a transparent material through which the user's fingerprint may be imaged by the imaging array.

46. A pointing device as recited in claim 42 wherein:

the fingerprint sensor includes a capacitive imaging array located at the particular button position contactable by the user's finger so that the user's fingerprint may be imaged by the capacitive imaging array.

47. A pointing device as recited in claim 46 wherein:

the fingerprint sensor is incorporated into an operable button located at the particular button position.

48. An apparatus comprising:

an electronic system requiring controlled access to certain capabilities and resources thereof;

a pointing device attached to said electronic system, said pointing device comprising

an interface for operably communicating with the electronic system;

a position sensor, responsive to user movement thereof, for conveying user positional information by way of said interface to the electronic system;

a user-depressable button for conveying user selection information by way of said interface to the electronic system; and

POINTING DEVICE WITH BIOMETRIC SENSOR

David J. Kinsella

ABSTRACT OF THE DISCLOSURE

A pointing device incorporates a biometric sensor at a location such that when operating the pointing device in a normal manner, a user's hand rests naturally in a position to place a finger of the user's hand in proximity to and readable by the biometric sensor. In one embodiment, a computer trackball pointing device includes a fingerprint sensor which is equally well suitable for use by either a right-handed or a left-handed user. Along with positional information from a position sensor and user selection information from at least one user-depressable button, the pointing device also conveys to an attached computer system information associated with the user's identity detected by the fingerprint sensor. Such a pointing device is well suited to both transparent verification as well as continuous verification, for if a user removes his or her hand from the natural position when using the device, the user's fingerprint will no longer be detectable by the fingerprint sensor, and the computer system to which the pointing device is attached can be alerted as to the need to re-authenticate any additional attempts at using the pointing device.

Fig. 1

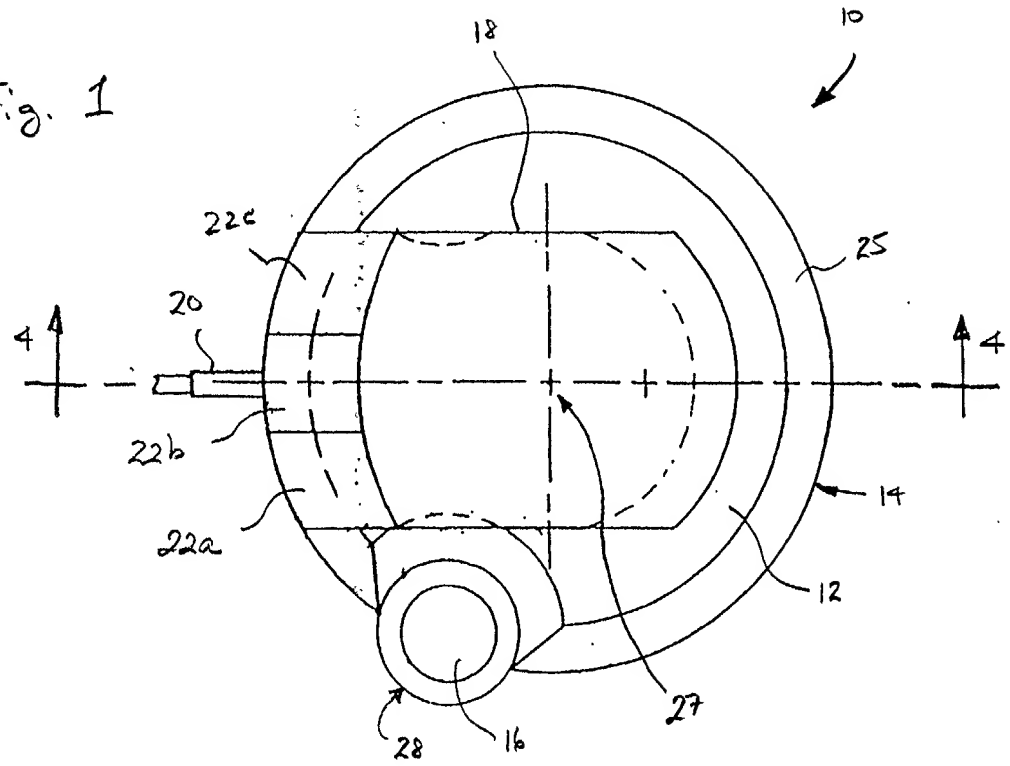


Fig. 3

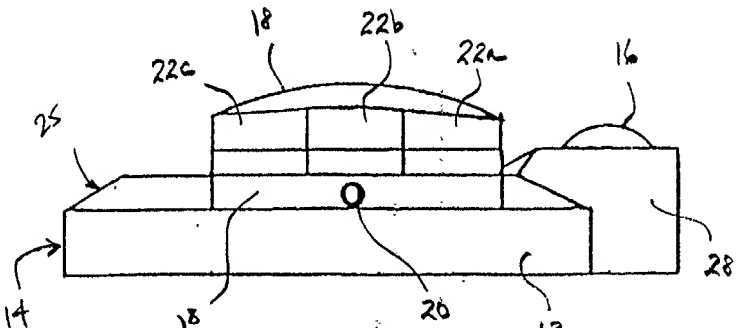


Fig. 3

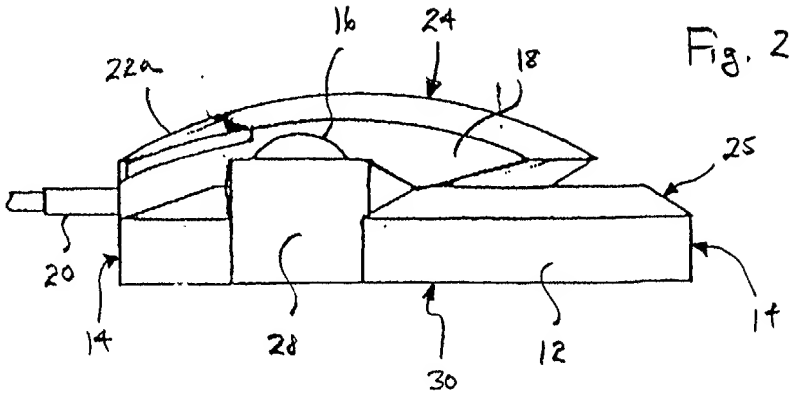
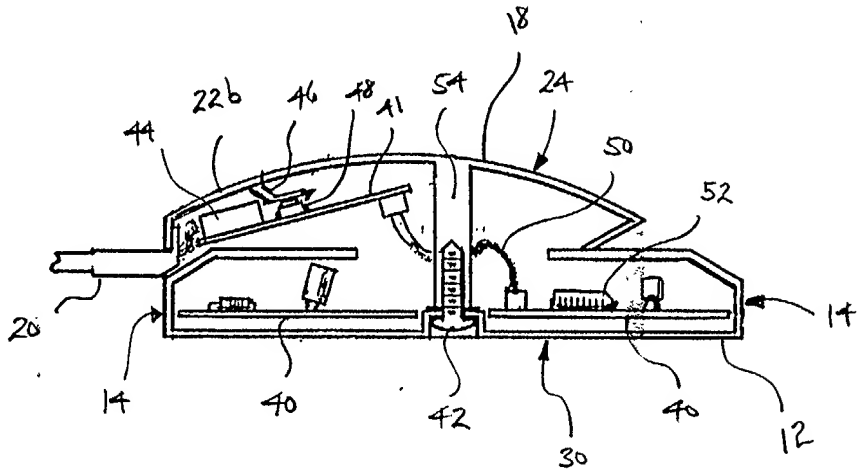


Fig. 2

Fig. 4



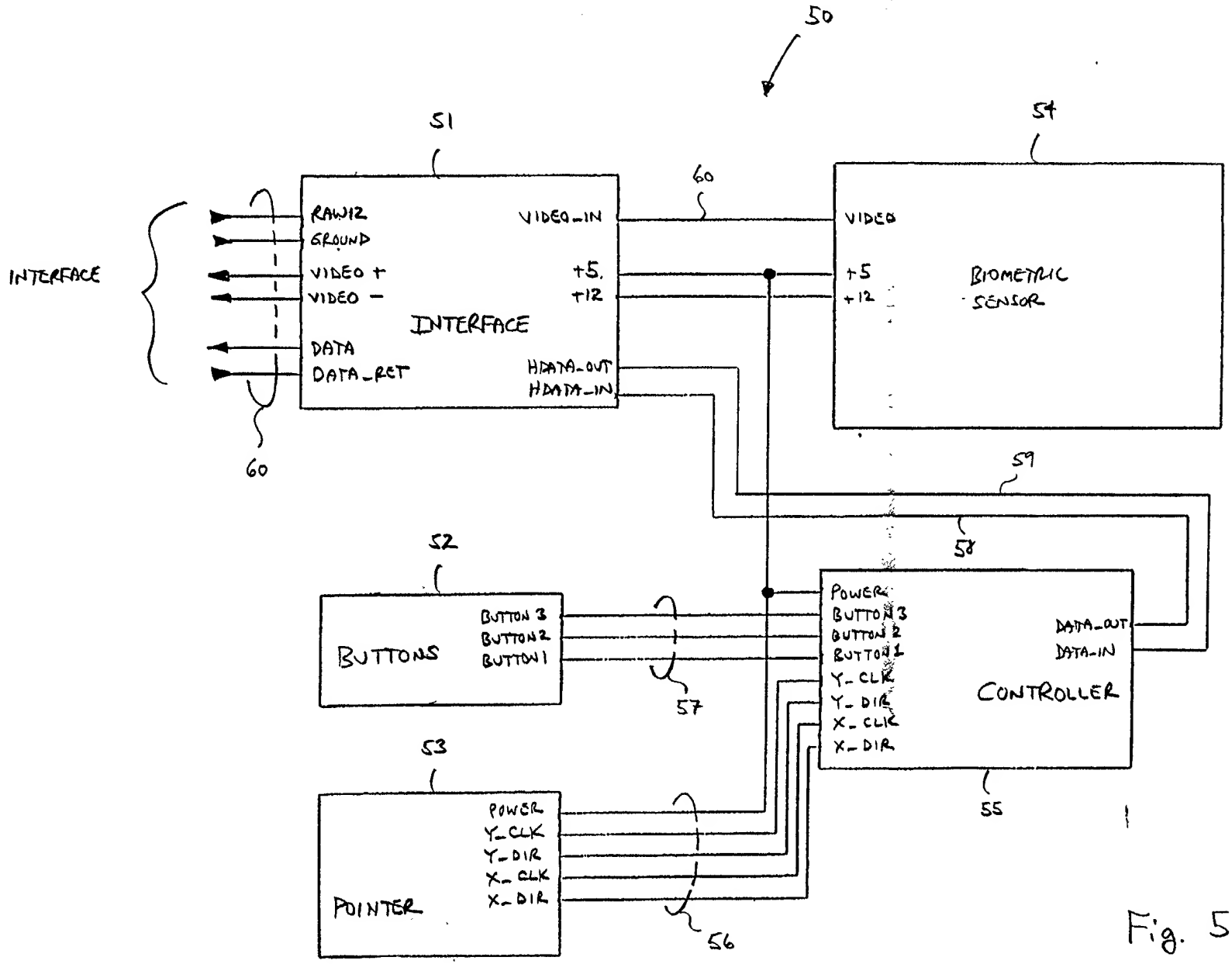


Fig. 5

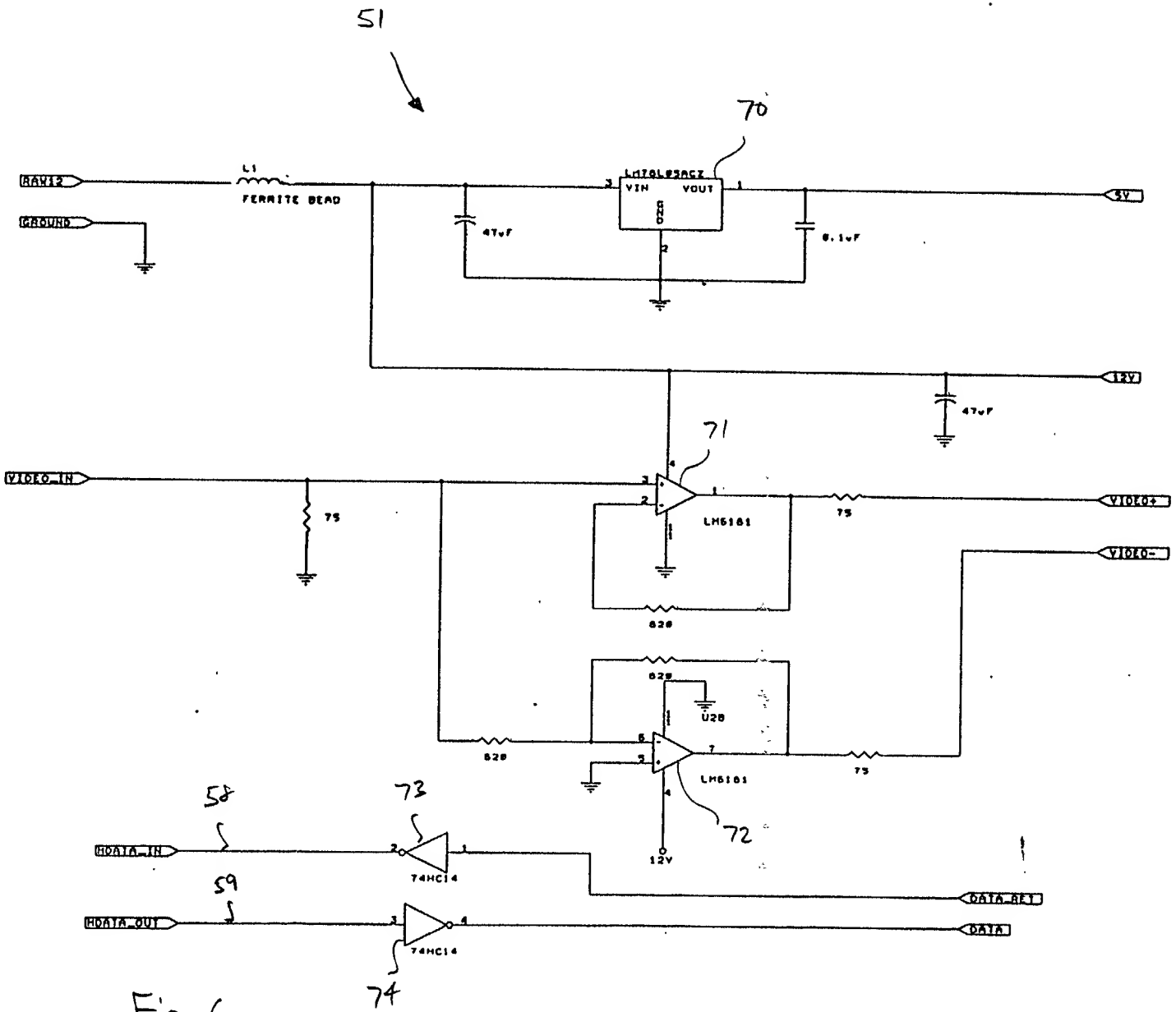


Fig. 6

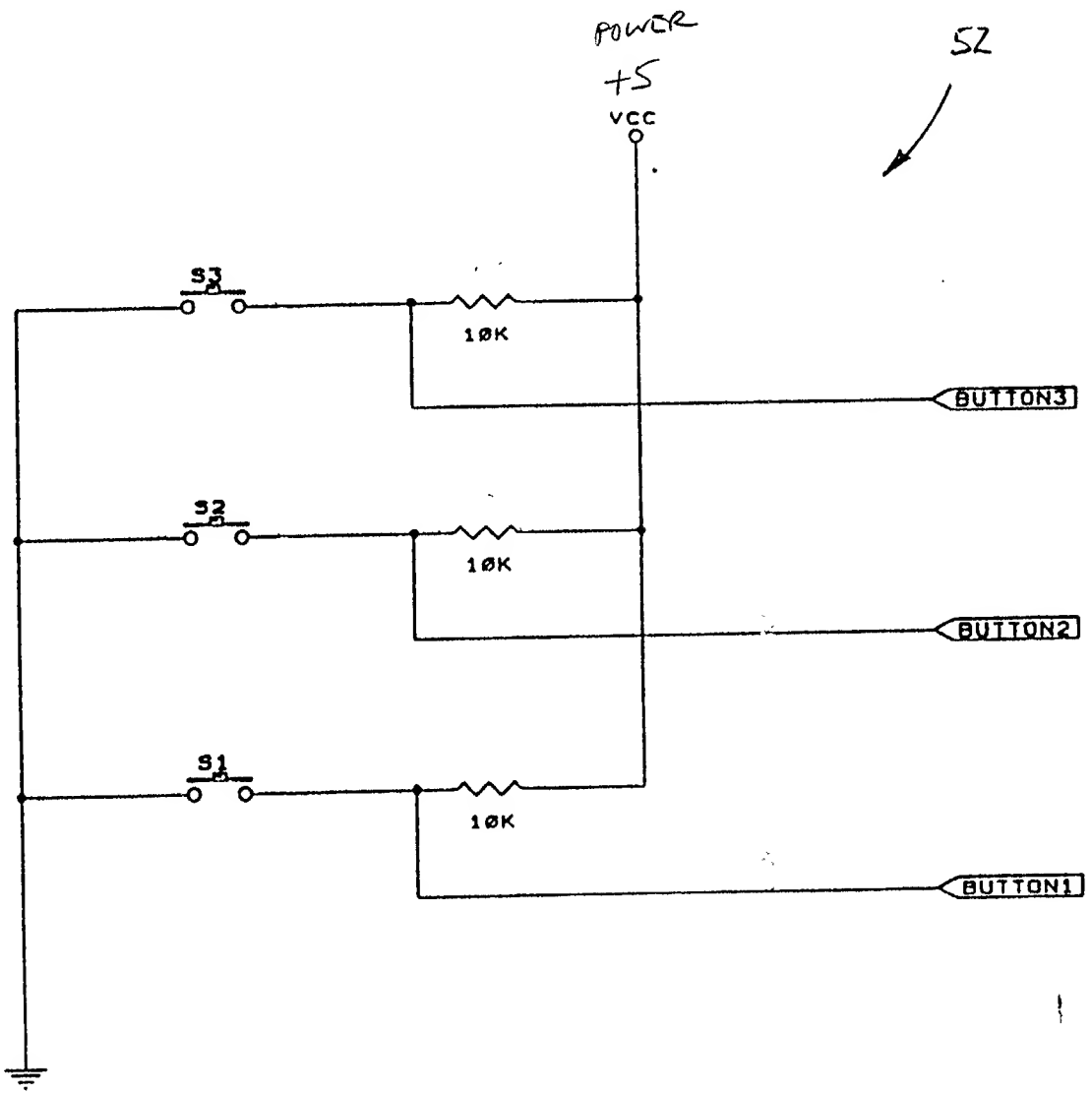


Fig. 7

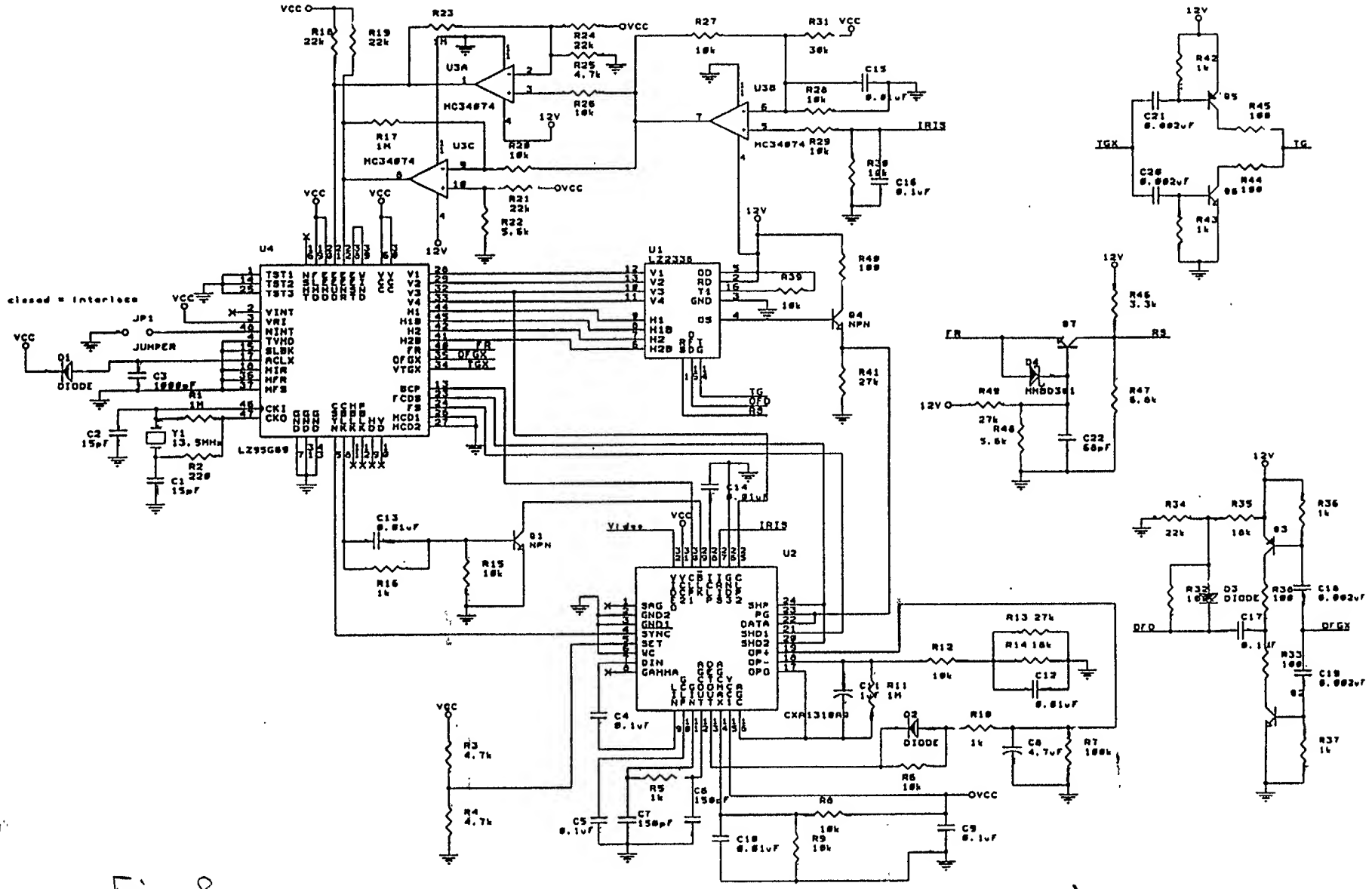

U4
LZ95G89
U1
LZ2336
U2
CXA1318AQ
U3A
U3B
U3C
HC34074
JP1
JUMPER
DIODE
Y1
13.5MHz
IRIS
Video
TG
DFD
DFGX
TGX
FR
Q1
Q2
Q3
Q4
NPN
DIODE
HM8036
12V
VCC
OVCC

Fig. 8

54

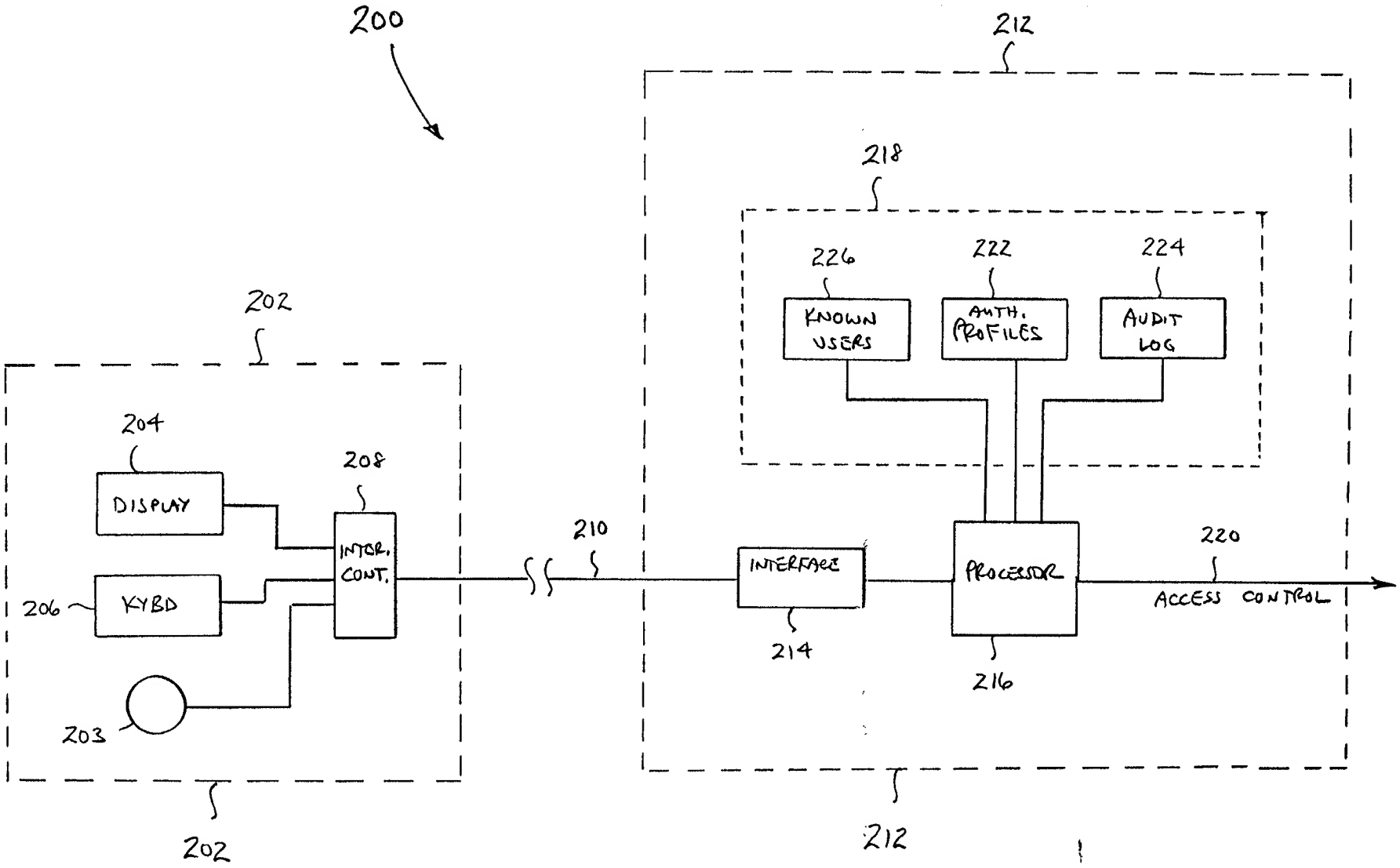

200
212
218
226
KNOWN USERS
222
AUTH. PROFILES
224
AUDIT LOG
202
204
DISPLAY
208
INTER. CONT.
206
KYBD
203
210
INTERFACE
214
PROCESSOR
216
220
ACCESS CONTROL
202
212

Fig. 9

DECLARATION FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below adjacent to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of subject matter (process, machine, manufacture, or composition of matter, or an improvement thereof) which is claimed and for which a patent is sought by way of the application entitled

POINTING DEVICE WITH BIOMETRIC SENSOR

which (check) ☒ is attached hereto.
☐ and is amended by the Preliminary Amendment attached hereto.
☐ was filed on ___ as Application Serial No. _____
☐ and was amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information, which is material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, § 119(a)-(d) of any foreign application(s) for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed:

Prior Foreign Application(s)			Priority Claimed	
Number	Country	Day/Month/Year Filed	Yes	No
N/A				

I hereby claim the benefit under Title 35, United States Code, § 119(e) of any United States provisional application(s) listed below:

Provisional Application Number	Filing Date
60/027,254	September 30, 1996

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s) listed below and, insofar as any subject matter of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose information, which is material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56, which became available between the filing date of the prior application(s) and the national or PCT international filing date of this application:

Application Serial No.	Filing Date	Status (patented, pending, abandoned)
N/A		

I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and to transact all business in the United States Patent and Trademark Office connected therewith:

Alan H. MacPherson (24,423); Thomas S. MacDonald (17,774); Kenneth E. Leeds (30,566); Brian D. Ogonowsky (31,988); David W. Heid (25,875); Guy W. Shoup (26,805); Forrest E. Gunnison (32,899); Norman R. Klivans (33,003); Edward C. Kwok (33,938); Patrick T. Bever (33,834); David E. Steuber (25,557); Michael Shenker (34,250); Laura Terlizzi (31,307); T. Lester Wallace (34,748); Ronald J. Meetin (29,089); Andrew C. Graham (36,531); Ken John Koestner (33,004); Stephen A. Terrile (32,946); Omkar K. Suryadevara (36,320); David T. Millers (37,396); E. Eric Hoffman (38,186); Kent B. Chambers (38,839); Emily M. Haliday (38,903); Serge J. Hodgson (40,017); David M. Sigmond (34,013); David W. O'Brien (40,107); M. Kathryn Braquet Tsirigotis (34,127); Mark Zagorin (36,067); Michael P. Adams (34,763); Bernard Berman (37,279); and Lawrence E. Lycke (38,540).

Please address all correspondence and telephone calls to:

Andrew C. Graham
SKJERVEN, MORRILL, MacPHERSON, FRANKLIN & FRIEL, L.L.P.
25 METRO DRIVE, SUITE 700
SAN JOSE, CALIFORNIA 95110

Telephone: (512) 794-3600
Facsimile: (512) 794-3601

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Title 18, United States Code, § 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of sole (or first joint) inventor: David J. Kinsella

Inventor's Signature: David J Kinsella Date: Sep 30, 1997
Residence: Austin, Texas Citizenship: USA
Post Office Address: 13614 Highway 71 West
Austin, Texas 78733

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:
David J. Kinsella

Serial No.: 08/940,553

Filed: September 30, 1997

For: POINTING DEVICE WITH BIOMETRIC SENSOR

Group Art Unit: 2723

Examiner: Vikkram, B.

Atty. Dkt. No.: KINS:002

POWER OF ATTORNEY

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

The undersigned, being the inventor named in the above-identified application, hereby revoke any previous Powers of Attorney and appoint:

Louis T. Pirkey, Reg. No. 22,393; Floyd R. Nation, Reg. No. 27,580; William D. Raman, Reg. No. 29,578; Richard J. Groos, Reg. No. 32,231; David L. Parker, Reg. No. 32,165; William G. Barber, Reg. No. 33,154; David D. Bahler, Reg. No. 30,932; Michael S. Metteauer, Reg. No. 34,875; Amber L. Hatfield, Reg. No. 36,824; Mark B. Wilson, Reg. No. 37,259; Steven L. Highlander, Reg. No. 37,642; Mark A. Thurmon, Reg. No. 39,858; G. Scott Thomas, Reg. No. 39,855; Teresa J. Bowles, Reg. No. 40,526; Stephen P. Meleen, Reg. No. 40,724; William W. Enders, Reg. No. 41,735; Mark J. Rozman, Reg. No. 42,117; Nicole Stafford, Reg. No. 43,929; Richard A. Nakashima, Reg. No. 42,023; Robert Hanson, Reg. No. 42,628; Michelle Muller; Reg. No. 42,913; Gina N. Shishima, Reg. No. 45,104; Chad Anson, Reg. No. P-44,510; Michael C. Barrett, Reg. No. P-44,523; Mark T. Garrett, Reg. No. P-44,699; Stephen J. Moloney, Reg. No. P-44,947; and Jonathan D. Hurt, Reg. No. P-44,790; and J. Paul Williamson, Reg. No. 29,600,

each an attorney or agent with the law firm of ARNOLD WHITE & DURKEE, as its attorney or agent so long as they remain with such law firm, with full power of substitution and revocation, to prosecute the application, to make alterations and amendments therein, to transact all business in the Patent and Trademark Office in connection therewith, and to receive any Letters Patent, and for one year after issuance of such Letters Patent to file any request for a certificate of correction that may be deemed appropriate.

Please direct all communications as follows:

Michael C. Barrett
ARNOLD WHITE & DURKEE
P.O. Box 4433
Houston, Texas 77210-4433
(512) 418-3000

Signature: David J. Kinsella Date: August 24, 1999

Name: David J. Kinsella